REMARKS

The fee for a three-month extension of time is provided herewith.

The claims were rejected as being unpatentable over a combination of Brown, Hwangbo and Sudia. Reconsideration and withdrawal of these rejections are respectfully requested, for the following reasons.

Each of the independent claims has been amended to recite:

> **accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;**

Indeed, the store of authority information that is accessed is a) stored apart from the payment request and b) is independent of the received certificate.

The Office points to Brown for a teaching of this claimed feature. Notably, the Office points to Figs. 1 and 3 and to paragraphs [0165], [0067], [0174] and [0183]. Examination of these figures and paragraphs, however, reveals that any "store of authority" in Brown is a) stored along with the document that is signed with the certificate and b) part of the certificate (so cannot be independent thereof).

Indeed, Fig. 1 clearly shows that the Role Identifier 104, the authenticator 100 and the digital signature 118 are an integral part of the document 102. Fig. 3 shows Brown's steps for digitally signing an electronic document – so any steps therein cannot be said to be stored apart from the payment request or independent of the certificate that signs the electronic document.

Paragraph [0067] states that the authenticator 100 is used to define the signer's authorization to sign the document 102:

> **[0067]** In one embodiment, the role identifier **104** includes an authenticator **110**, which is used to authenticate the signer's identity, as well as the signer's authorization to sign the document **102** in the specified role. Although a variety of authentication systems exist, a public key cryptosystem is preferably used to authenticate the signer, as described hereafter. In one embodiment, the authenticator **110** is implemented as a "plug-in" module to a conventional Web browser. Although the authenticator **110** is illustrated herein as a component of the role identifier **104**, it should be recognized that the authenticator **110** could be implemented as a separate functional unit.

Therefore, the authorization of Brown is contained in the document 102 (which, according to Brown, may be a payment request) itself. Brown's documents, therefore, are self-authenticating (subject to verification of the certificate itself with the Certificate Authority) and **self-authorizing**, as the authority of the signer is contained within the document itself.

The present inventions specifically address this issue, by a) separating identity and authority and b) by accessing a store of authority that is stored apart from the document in question and that is independent of the received certificate.

Paragraph [0165] detail digital certificates and does not teach or suggest accessing any store of authority information that is separate from the document (e.g., payment request) and that is independent of the certificate itself:

> **[0165]** In general, digital certificates contain the name of the subscriber, the subscriber's public key, the digital signature of the issuing CA, the issuing CA's public key, and other pertinent information about the subscriber and his organization, such as his authority to conduct certain transactions. These certificates are stored in an on-line, publicly accessible repository, and are accessed using a standard protocol, such as the Lightweight Directory Access Protocol (LDAP). As noted earlier, these certificates are preferably stored in the document **102** near the associated digital signature **118**. The repository also maintains an up-to-date listing of all the unexpired certificates which have been revoked, referred to as a Certificate Revocation List (CRL).

Consistent with the above-described approach, Brown's paragraph [0174] teaches the request for payment is authorized based upon the authority of the signer which, as taught in Figs. 1 and 3, is contained with the signed document 102 itself:

> **[0174]** Thus, in one embodiment, the payment processing service **712** checks a document **102** for an electronic payment request, authorizes the request based on the authority of the signer, and completes the electronic payment. A significant advantage over conventional electronic payment systems is that the electronic payment request is authorized by a digital signature **118**, making the request non-repudiatable.

Lastly, the Office relied upon paragraph [0183]:

> **[0183]** If, however, the signature was successfully verified, the method continues by checking **886** the digital certificate corresponding to the signature **118** for the maximum signing authority of the signer. Under X.509 version 3, the digital certificate may specify a maximum signing authority. For example, a signer may only be authorized to digitally sign payment requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00.

As is made clear herein, the authority (e.g., the maximum that the signer can authorize) is checked by checking (at 886) the digital certificate corresponding to the signature 118. Therefore, Brown clearly tells us that the authority is most assuredly not independent of the certificate, but an integral part thereof (in that the authority that is checked is stored within the certificate itself). This is in direct contrast to the claimed embodiments, in which the store of authority that is accessed is stored separately from the received payment request and is independent of the received certificate, both of which are untaught and unsuggested by Brown. Kindly note that information stored by the Certificate Issuing Authority (commonly abbreviated as CA) in Brown or any other reference is, by definition, directly associated with the certificate, and cannot be said to be independent of the certificate.

This shortcoming of Brown is not remedied by either Hwangbo or Sudia. In Hwangbo, paragraph [0029] details the creation of the public and private key pair, which are required to create the certificate. Paragraph [0034] details the extension fields defined by the X.509 standard, as does paragraph [0096], Fig. 10 and claim 17 noted in the outstanding Office Action. Hwangbo, therefore, does not teach any step of accessing a store of authority information that is separate from the document (e.g., payment request) or independent of the certificate (quite to the contrary, the certificate itself is relied on and trusted as the sole source of authority, as it is in Brown).

Turning now to Sudia, paragraph [0132], contrary to what is asserted on page 6 of the outstanding Office Action, does not teach accessing a store of authority information that is independent of the received certificate:

> [0132] **FIGS. 7 and 8** illustrate steps for certifying and registering authorizing agents. **FIG. 7** shows an overall system architecture, while **FIG. 8** illustrates the processing sequence for a certification request. Signing devices will affix the system wide authority official signature to authorizing agent certificates, thus certifying a public signature verification key for each authorizing agent. In the registration process, each signing device will also update an internally-stored table of particular authorizing agents who will be empowered to instruct the signing device to apply its partial signature. During routine operation, a signing device will affix its partial signature only if the request is signed by a minimum number of temporarily certified or SWA certified authorizing agents (or if a minimum number of individually signed messages are receives) as discussed more fully below. An example of the process for certifying Authorizing Agent 3*a* (AA3*a*) and registering AA3*a* with Signing Device 3 proceeds as follows.

What paragraph [0132] does say, is that Figs. 7 and 8 show steps for certifying and registering authorizing agents. Therefore, Figs. 7 and 8 detail who the agents are and how they are authorized. Lines 5-7 tell us that signing devices affix a system wide authority signature to certificates, which involves identity (and not authority, even when applying an authority signature) and certificates. This certifies a public signature verification key for each authorizing agent. See lines 6-7. Lines 8-12 detail the manner in which each signing device updates the table of agents

who are empowered to instruct the signing device to apply its partial signature. Again, this table details who is authorized, which is a question of identity, not authority. The remainder of this passage details the conditions under which a signing device may affix its partial signature, and at no point is there any disclosure or suggestion of accessing a store of authority that is separate from a received payment request and/or independent of a received certificate.

Paragraph [0171] (too long to be reproduced herein in its entirety) details "a command 213 adding an authorized agent". Thus, this paragraph details Sudia's steps for adding an authorized agent. Item d) in the command 213 for adding an authorizing agent states that the command includes an administrative class 225 indicating the powers for which the agent is authorized. However, item h) states that a certificate 231 is included with the trusted device's public key and that the certificate 231 is included with the command 231:

> **229** of the agent's trusted device; and h) a certificate **231** with the trusted device's public signature verification key. Preferably, the pubic key of the new agent is certified **233** under the authority of the SWA signature key and the certificate is included with the command. The device cer-

Therefore, Sudia is yet another example (consistent with Brown and Hwangbo), in which the authority information is coupled to the document with included certificate (Brown), X.509 certificate (Hwangbo). In Sudia's case, the authority is included with the command 231 (making the command self-authorizing in the same manner as the documents of Brown and Hwangbo were also self-authorizing) to add another authorizing agent who will be given the authority to direct a signing device to affix its partial signature. In direct contrast, the store of authority information, as claimed, is stored separate from and independent of the received certificate. Therefore, the claimed embodiments do not rely on a proffered document, certificate or command for the last word on the authority of the person proffering the document or certificate. Instead, that indication of authority

is checked against a separate and independent source by accessing the claimed store of information that is separate from and independent of the received certificate, as claimed herein.

Paragraph [0252] of Sudia merely states that...

> device as discussed above. Upon receipt of the signature request, the primary user's card will verify that the requesting user's signature(s) match(es) the public key(s) tat were originally specified in the substitution certificate, apply the primary user's signature **419**, and forward the signed document on to a signing device **421** (or other destination) in the usual manner.

...meaning that upon receipt of a signature request, the signature in the request is matched against the certificate's public key (making it hardly independent of a certificate), whereupon the primary user's certificate may be applied and the document forwarded to a signing device 412. No teaching or suggestion of any accessing step as claimed herein is present in this passage or the remainder of Sudia.

Considering now the Brown, Hwangbo and Sudia references in combination, it becomes clear that, to the extent that they teach or suggest authority information, such authority information is invariably tied to, stored along with, and dependent upon a certificate that is used as the primary means of verifying the authenticity/validity of a document, command or the identity of an authorizing agent. The applied combination is not believed to teach or to suggest any step of

> **accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate;**

alone or in combination with the remaining steps of the claimed methods or apparatus. In view of the present amendments to the claims and the arguments present herein, it is respectfully submitted that the applied combination does not teach or suggest the currently claimed

embodiments. Reconsideration and withdrawal of the 35 USC §103(a) rejections are respectfully requested.

Applicant believes that this application is now in condition for allowance. If any unresolved issues remain, please contact the undersigned attorney of record at the telephone number indicated below and whatever is necessary to resolve such issues will be done at once.

Respectfully submitted,

Date: December 24, 2008 By: _____

Alan W. Young
Attorney for Applicant
Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

C:\YLF\CLIENTS\ORCL\5881 (OID-2003-142-01)\5881 AMEND.6.doc